DISEÑO DE UNA METODOLOGÍA PARA REALIZAR DIAGNÓSTICO AL ESTADO DE GOBIERNO DE TI EN UNA ORGANIZACIÓN FUNDAMENTADO EN LOS LINEAMIENTOS ESTABLECIDOS POR LOS ESTANDARES RECONOCIDOS COMO LAS MEJORES PRÁCTICAS

DERLYS KATHERINE NAVAS LINEROS

CORPORACIÓN UNIVERSITARIA DE LA COSTA (C.U.C.)
FACULTAD DE CONTADURIA PÚBLICA
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE INFORMACIÓN
BARRANQUILLA
2011

DISEÑO DE UNA METODOLOGÍA PARA REALIZAR DIAGNÓSTICO AL ESTADO DE GOBIERNO DE TI EN UNA ORGANIZACIÓN FUNDAMENTADO EN LOS LINEAMIENTOS ESTABLECIDOS POR LOS ESTANDARES RECONOCIDOS COMO LAS MEJORES PRÁCTICAS

DERLYS KATHERINE NAVAS LINEROS

Proyecto de grado

Asesor
Víctor Manuel Montaño Ardila
Especialista en auditoria de sistemas

CORPORACIÓN UNIVERSITARIA DE LA COSTA (C.U.C.)
FACULTAD DE CONTADURIA PÚBLICA
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE INFORMACIÓN
BARRANQUILLA
2011

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

DEDICATORIA

A Dios por ser mi soporte y fortaleza.

A mis padres por su apoyo y ejemplo de perseverancia.

A mi esposo por ser mi polo a tierra.

A mi hija por ser mi motivación.

A mis docentes por ser mi guía.

A mi tutor por su apoyo y colaboración.

A mis compañeros de especialización por sus conocimientos y apoyo incondicional.

Derlys Navas Lineros

TABLA DE CONTENIDO

LISTA DE IMÁGENES pág.

RESUMEN

Hoy en día la gran mayoría de los procesos de las organizaciones se encuentran soportados en tecnología de la información. A su vez, la información se ha convertido en el activo más importante dentro de las organizaciones. Por ello la gestión de los recursos de tecnología que soportan los procesos organizacionales es una necesidad apremiante para las organizaciones.

Se han desarrollado diversos estándares y normas para gestionar los recursos y servicios informáticos y garantizar la seguridad de la información de la organización. Estas normas son de libre implementación, por ello, muchas veces se aplican de forma errada generando pérdidas para las organizaciones. El diseño e implementación de un modelo de gobierno de TI se ha convertido casi que en una obligación para toda organización que quiera lograr el éxito.

En este proyecto se propone una metodología para diagnosticar el estado actual del gobierno de TI de una organización con el fin de conocer el nivel de madurez y cumplimiento de la organización con respecto al modelo que ha establecido. Para el desarrollo de la misma se toma como base el marco de referencia COBIT a partir de estos se diseño un instrumento de levantamiento de información sencillo que permitirá valorar de forma general el modelo de gobierno de cualquier organización.

La metodología propuesta consta de 8 fases partiendo del conocimiento de la organización y su entorno, siguiendo por la selección de referentes conceptuales que serán utilizados en la creación del instrumento de levantamiento de la

organización. La organización deberá establecer un esquema de puntuación y unas métricas para valorar los resultados de la aplicación del instrumento. Luego de la aplicación del instrumento y su valoración se procederá a establecer la brecha existente entre el estado actual de la organización y su estado deseado y entre el estado de la organización y el de su entorno. El diagnostico permitirá definir e implementar las actividades y procedimientos necesarios para lograr alcanzar el nivel deseado por la organización.

SUMMARY

Today the vast majority of organizational processes are supported in information technology. In turn, information has become the most important asset in organizations. Thus the management of technology resources that support organizational processes is a pressing need for organizations.

They have developed different standards and rules to manage computing resources and services and ensuring the security of organizational information. These standards are free implementation, therefore, often applied in the wrong way for organizations to generate losses. The design and implementation of an IT governance model that has become almost a must for any organization that wants to succeed.

This project proposes a methodology to diagnose the current state of IT governance in an organization to know the level of maturity and performance of the organization with respect to the model set. For the development of it is taken based on the COBIT framework from these an instrument was designed to gather information that will evaluate simple generally the governance of any organization.

The proposed methodology consists of 8 phases from knowledge about the organization and its environment, following the selection of conceptual references that will be used in creating the survey instrument of the organization. The organization shall establish a scoring scheme and a metric to assess the results of applying the instrument. After application of the instrument and its evaluation will proceed to establish the gap between the current state of the organization and its

desired state and between the state of the organization and its environment. The diagnosis will define and implement activities and procedures necessary to achieve the desired level by the organization.

INTRODUCCIÓN

El uso de las tecnologías de la información en la ejecución de los procesos definidos dentro de las organizaciones es cada vez más elevado, convirtiéndose estas en el soporte de los procesos misionales de la compañía. Por ello, ha surgido la necesidad de gestionar los recursos y servicios informáticos de la organización de forma eficiente en respuesta a los requerimientos regulatorios y operativos aplicables a esta.

Las situaciones descritas anteriormente han generado en las organizaciones la necesidad de establecer un modelo gobierno de tecnologías de la información que permitan cumplir los objetivos estratégicos de las estas a través del uso de las mejores prácticas para la toma de decisiones gerenciales con respecto a TI.

Los lineamientos establecidos en el modelo de gobierno propuesto por la organización se ven afectados por factores externos e internos. Por ello, en el presente trabajo se diseñara una metodología que permitirá diagnosticar el estado actual del modelo de gobierno de TI de una organización con el fin de establecer las acciones necesarias para garantizar el cumplimiento de las metas propuestas por la organización.

1. PLANTEAMIENTO DEL PROBLEMA

El cumplimiento de los objetivos estratégicos de una organización determina el éxito de esta en el mercado. Por ello, las organizaciones hacen uso del gobierno corporativo para lograr dichos objetivos mediante una apropiada administración los recursos corporativos y una adecuada gestión de los riesgos a los que se encuentran expuestos sus procesos.

Actualmente, la alta dirección de las organizaciones se ha dado cuenta de la importancia de las tecnologías de la información como herramienta de apoyo a sus procesos y de la influencia de estas en la consecución de los objetivos organizacionales y por ende del éxito de la organización. Es por ello, que las compañías han adoptado estándares como mecanismos que les permitan administrar o gobernar los recursos de tecnología de la información.

Existe una gran cantidad de estándares y normas que sirven como guía para la implementación de un adecuado gobierno de tecnologías de la información. Sin embargo, la carencia de conocimiento de las organizaciones, su poca capacidad de adaptabilidad y respuesta ante las exigencias del mercado con referencia a la gobernabilidad de las tecnologías de la información y la falta de personal idóneo para la ejecución de un plan estratégico de TI han generado en algunos casos una mala interpretación de estos estándares y por consiguiente una errada implantación de los mismos

Este fenómeno se presenta en una gran cantidad de organizaciones a nivel mundial, afectando la eficiencia y eficacia de los procesos apoyados en TI y por

consiguiente los intereses económicos de la organización, debido a la inadecuada implantación de su modelo de gobierno de TI.

Por lo anteriormente expuesto cabe preguntarnos:

¿Qué estándares considerados como “mejores prácticas” proporcionan lineamientos válidos para la construcción de un adecuado modelo de Gobierno de TI?

¿Es factible diseñar una metodología para realizar un diagnóstico del estado de cumplimiento del modelo de Gobierno de TI de una organización con respecto a sus requerimientos de crecimiento y consolidación?

2. JUSTIFICACIÓN

Para muchas organizaciones la adopción de estándares y normas para la implementación de un modelo de gobierno de TI se ha convertido en su mejor arma para la consecución de sus objetivos estratégicos. Asimismo, la naturaleza general de estas normas y estándares permiten a las organizaciones adoptarlos de acuerdo a sus necesidades y propósitos estratégicos. Esta situación ha generado en un gran número de casos una inadecuada implementación de estas normas y estándares partiendo de una errada selección de las mismas con respecto a la naturaleza y estrategia de la organización, la falta o inadecuada definición de métricas e indicadores que permitan medir los resultados de dicha implantación. Por ello, se ha considerado trascendente diseñar una metodología que permita diagnosticar el estado de gobierno de tecnologías de la información de una organización.

El estudio planteado ayudara a las organizaciones a medir su nivel de cumplimiento con respecto a lo que indican los estándares y normas más conocidas y adoptadas por las organizaciones a nivel mundial para la construcción de sus modelos de gobierno de TI. La investigación es viable ya que se dispone de los recursos necesarios para su desarrollo.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Diseñar una metodología para realizar diagnostico al estado de gobierno de TI en una organización fundamentado en los lineamientos establecidos por los estándares reconocidos como las mejores prácticas.

3.2. OBJETIVOS ESPECIFICOS

Identificar y seleccionar los referentes conceptuales que proveerán lineamientos para la construcción del modelo (estándares, industria y académicos).

Diseñar un instrumento de recolección de información que permita determinar el estado actual de gobierno TI de una organización.

4. DELIMITACIÓN

4.1. DELIMITACIÓN TEMPORAL

El presente proyecto se realizara en el período comprendido entre Julio y Octubre de 2011. Durante este período se cumplieron una serie de fases que se encuentran detalladas en el cronograma de actividades.

4.2. DELIMITACIÓN TÉCNICA

Para este estudio se hizo uso de las siguientes normas y estándares:

- COBIT 4.1
- ISO 27002:2005
- ITIL V3

5. MARCO TEÓRICO

5.1. COBIT

COBIT (Control OBjectives for Information and related Technology | Objetivos de Control para tecnología de la información y relacionada) es un marco de referencia mundialmente aceptado para el gobierno y gestión de las tecnologías de la información. Fue desarrollado por la Information Systems Audit and Control Association (ISACA) en asocio con el IT Governance Institute (ITGI).

Este marco de referencia ofrece un conjunto de mejores prácticas para garantizar la alineación de las tecnologías de la información con los objetivos del negocio, el uso eficiente de los recursos tecnológicos, la administración adecuada de los riesgos y el aumento de los beneficios del negocio mediante el uso de las tecnologías de la información.

De igual forma, define como responsables del gobierno de tecnologías de la información a la junta directiva y ejecutivos de la organización. Así mismo, define 5 áreas de enfoque en las cuales los ejecutivos deben colocar atención para realizar una adecuada gobernabilidad de las tecnologías de la información (Figura 1).

Figura 1. Áreas de enfoque del Gobierno de TI - Tomada de COBIT 4.1

COBIT tiene como misión “Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento.”[1] y se basa en el siguiente como principio “Para proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita invertir en, y administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que provean los servicios que entregan la información empresarial requerida”[2] (Figura 2).

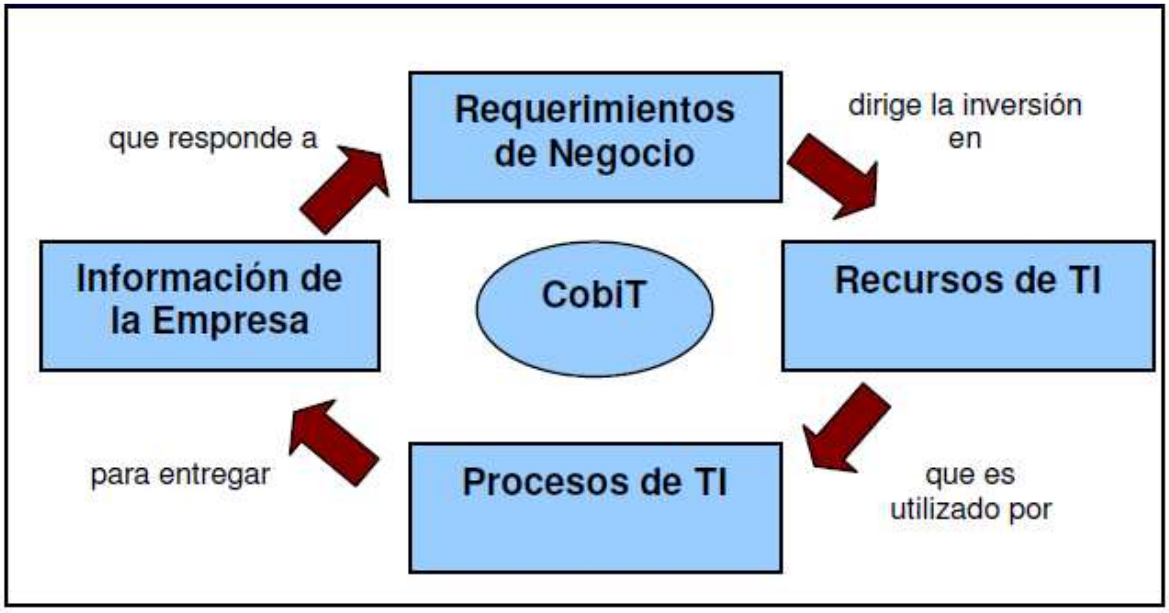

Figura 2. Principio básico de COBIT - Tomada de COBIT 4.1

Para el cumplimiento de los requerimientos de la organización COBIT define recursos de tecnologías de la información en los cuales la organización debe invertir y velar por su buen funcionamiento. Estos recursos son:

Las personas: compuesto por el recurso humano necesario para gestionar los servicios y recursos de TI.

[1] COBIT 4.1
[2] COBIT 4.1

La infraestructura: compuesto por el Hardware y software que soportan las aplicaciones.
La información: compuestos por los datos en todas sus formas, ingresados, procesados o generados por los sistemas de información.
Las aplicaciones: compuestos por sistemas automatizados y procedimientos manuales para el procesamiento de información.

Para la consecución de los objetivos de la organización COBIT define 7 criterios que la información debe cumplir estos son:

Eficiencia: la información debe ser generada de manera óptima.
Efectividad: la información debe ser pertinente y relevante para la organización.
Confidencialidad: la información sensible de la organización debe ser conocida y manipulada por personal autorizado.
Integridad: la información deber ser precisa, completa y exacta.
Disponibilidad: la información debe estar disponible en el momento en que cualquier proceso de la organización lo requiera.
Cumplimiento: la información debe satisfacer las regulaciones y leyes aplicables a la organización
Confiabilidad: la información entregada a la alta gerencia debe ser apropiada.

Para gobernar adecuadamente TI se deben establecer actividades y procedimientos que deben ser gestionados, COBIT agrupa estas actividades en 4 dominios, que son:

Planear y Organizar: en este dominio se cubre todo lo referente a la alineación de las tecnologías de la información con los objetivos del negocio. Definiendo una estrategia que permita a la organización hacer uso de los recursos tecnológicos en pro del óptimo funcionamiento de sus procesos. Se subdivide en 10 procesos:

- PO1 Definir un Plan Estratégico de TI
- PO2 Definir la Arquitectura de la Información
- PO3 Determinar la Dirección Tecnológica
- PO4 Definir los Procesos, Organización y Relaciones de TI
- PO5 Administrar la Inversión en TI
- PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia
- PO7 Administrar Recursos Humanos de TI
- PO8 Administrar la Calidad
- PO9 Evaluar y Administrar los Riesgos de TI
- PO10 Administrar Proyectos

Adquirir e Implementar: este dominio cubre la identificación, adquisición, implementación y mantenimiento de las soluciones y recursos de TI necesarios para el cumplimiento del plan estratégico de TI. Se subdivide en 7 procesos:

- AI1 Identificar soluciones automatizadas
- AI2 Adquirir y mantener software aplicativo
- AI3 Adquirir y mantener infraestructura tecnológica
- AI4 Facilitar la operación y el uso
- AI5 Adquirir recursos de TI
- AI6 Administrar cambios
- AI7 Instalar y acreditar soluciones y cambios

Entregar y Dar soporte: este dominio cubre la entrega de los servicios requeridos por la organización y el soporte de las aplicaciones y recursos de TI en general. Se subdivide en 13 procesos:

- DS1 Definir y administrar los niveles de servicio
- DS2 Administrar los servicios de terceros

- DS3 Administrar el desempeño y la capacidad
- DS4 Garantizar la continuidad del servicio
- DS5 Garantizar la seguridad de los sistemas
- DS7 Educar y entrenar a los usuarios
- DS6 Identificar y asignar costos
- DS8 Administrar la mesa de servicio y los incidentes
- DS9 Administrar la configuración
- DS10 Administrar los problemas
- DS11 Administrar los datos
- DS12 Administrar el ambiente físico
- DS13 Administrar las operaciones

Monitorear y Evaluar: este dominio cubre la revisión continua y administración del desempeño de los recursos de TI. Así como el monitoreo y evaluación del control interno, el cumplimiento de las regulaciones aplicables a la organización y la administración del gobierno de TI. Se subdivide en 4 procesos:

- ME1 Monitorear y Evaluar el Desempeño de TI
- ME2 Monitorear y Evaluar el Control Interno
- ME3 Garantizar el Cumplimiento Regulatorio
- ME4 Proporcionar Gobierno de TI

COBIT cuenta con un modelo de madurez compuesto por 6 Niveles que van de 0 a 5 (Figura 3). Este modelo permite evaluar el nivel de cumplimiento de la organización con respecto a los objetivos de control que esta haya adoptado. Cada uno de los procesos de COBIT puede ser evaluado a través de este sistema dando como resultado las condiciones actuales de la organización, lo que le permitirá realizar comparaciones con sus organizaciones de su mismo entorno. De igual forma, le permitirá a la organización elegir el nivel de madurez en el que desea estar a futuro y determinar la brecha entre su estado actual y el deseado. A

partir de estos resultados la organización definirá la estrategia y procedimientos a seguir para llegar a su estado deseado.

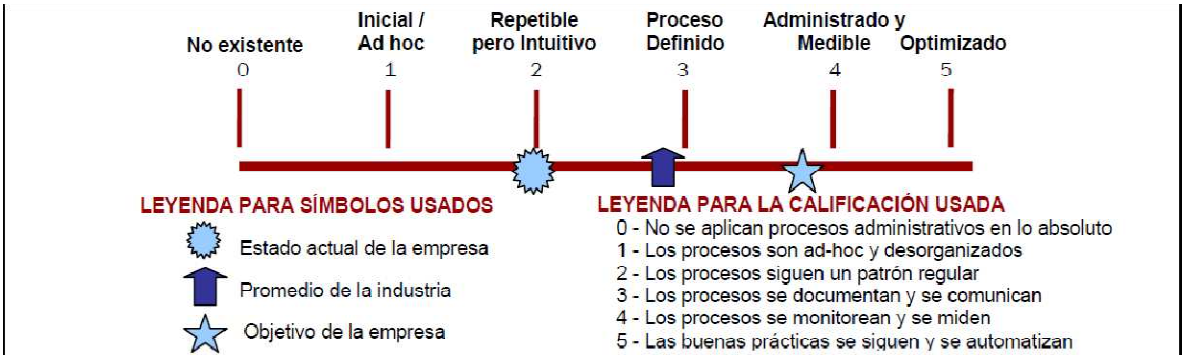

Figura 3. Representación gráfica del modelo de madurez COBIT - Tomada de COBIT 4.1

5.2. ISO 27002:2005

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

ISO 27002 es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, está compuesta por los objetivos de control y controles que podrán seleccionar las organizaciones para la creación y gestión de su sistema de seguridad de la información. No todos los objetivos de control son de obligatorio cumplimiento ya que depende de las condiciones del negocio. Sin embargo el no cumplimiento de un objetivo de control debe ser justificable.

La norma no sólo cubre la problemática de la seguridad IT sino que hace una aproximación holística a la seguridad de la información corporativa, abarcando

todas las actividades de una organización en lo referente a la seguridad de la información que maneja.

Esta norma permite gestionar la seguridad de la información y por consiguiente la continuidad de los procesos en la que esta es participe en cualquiera de sus estados. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Los 11 dominios de ISO 27002:2005 son:

- Política de seguridad: documento de política de seguridad y su gestión. Los objetivos de control de este dominio son:
    - Política de seguridad de la información.
- Aspectos organizativos de la seguridad de la información: organización interna; terceros. Los objetivos de control de este dominio:
    - Organización interna.
    - Terceros.
- Gestión de activos: responsabilidad sobre los activos; clasificación de la información. Los objetivos de control de este dominio son:
    - Responsabilidad sobre los activos.
    - Clasificación de la información.
- Seguridad ligada a los recursos humanos: antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo. Los objetivos de control de este dominio son:
    - Antes del empleo.
    - Durante el empleo.
    - Cese del empleo o cambio de puesto de trabajo.
- Seguridad física y ambiental: áreas seguras; seguridad de los equipos. Los objetivos de control de este dominio son:
    - Áreas seguras.
    - Seguridad de los equipos.
- Gestión de comunicaciones y operaciones: responsabilidades y procedimientos de operación; gestión de la provisión de servicios por

terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión. Los objetivos de control de este dominio son:

  - Responsabilidades y procedimientos de operación.
  - Gestión de la provisión de servicios por terceros.
  - Planificación y aceptación del sistema.
  - Protección contra el código malicioso y descargable.
  - Copias de seguridad.
  - Gestión de la seguridad de las redes.
  - Manipulación de los soportes.
  - Intercambio de información.
  - Servicios de comercio electrónico.
  - Supervisión.

- Control de acceso: requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo. Los objetivos de control de este dominio son:
  - Requisitos de negocio para el control de acceso.
  - Gestión de acceso de usuario.
  - Responsabilidades de usuario.
  - Control de acceso a la red.
  - Control de acceso al sistema operativo.
  - Control de acceso a las aplicaciones y a la información.
  - Ordenadores portátiles y teletrabajo.
- Adquisición, desarrollo y mantenimiento de los sistemas de información: requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos; seguridad de los archivos de

sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica. Los objetivos de control de este dominio son:

  - Requisitos de seguridad de los sistemas de información.
  - Tratamiento correcto de las aplicaciones.
  - Controles criptográficos.
  - Seguridad de los archivos de sistema.
  - Seguridad en los procesos de desarrollo y soporte.
  - Gestión de la vulnerabilidad técnica.

- Gestión de incidentes de seguridad de la información: notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras. Los objetivos de control de este dominio son:
  - Notificación de eventos y puntos débiles de seguridad de la información.
  - Gestión de incidentes y mejoras de seguridad de la información.
- Gestión de la continuidad del negocio: aspectos de la seguridad de la información en la gestión de la continuidad del negocio. Los objetivos de control de este dominio son:
  - Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
- Cumplimiento: cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información. Los objetivos de control de este dominio son:
  - Cumplimiento de los requisitos legales.
  - Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.
  - Consideraciones sobre las auditorías de los sistemas de información.

5.3. ITIL V3.0

Es un conjunto de de mejores prácticas para la gestión y soporte de servicios de TI. Busca garantizar la continuidad del negocio a través de una adecuada gestión de los servicios informáticos externos e internos desde su parte financiera hasta su parte técnica y el soporte de dichos servicios. ITIL alinea los servicios de TI con los requerimientos del negocio, no está atado a ninguna tecnología en particular y puede ser adoptado por cualquier organización.

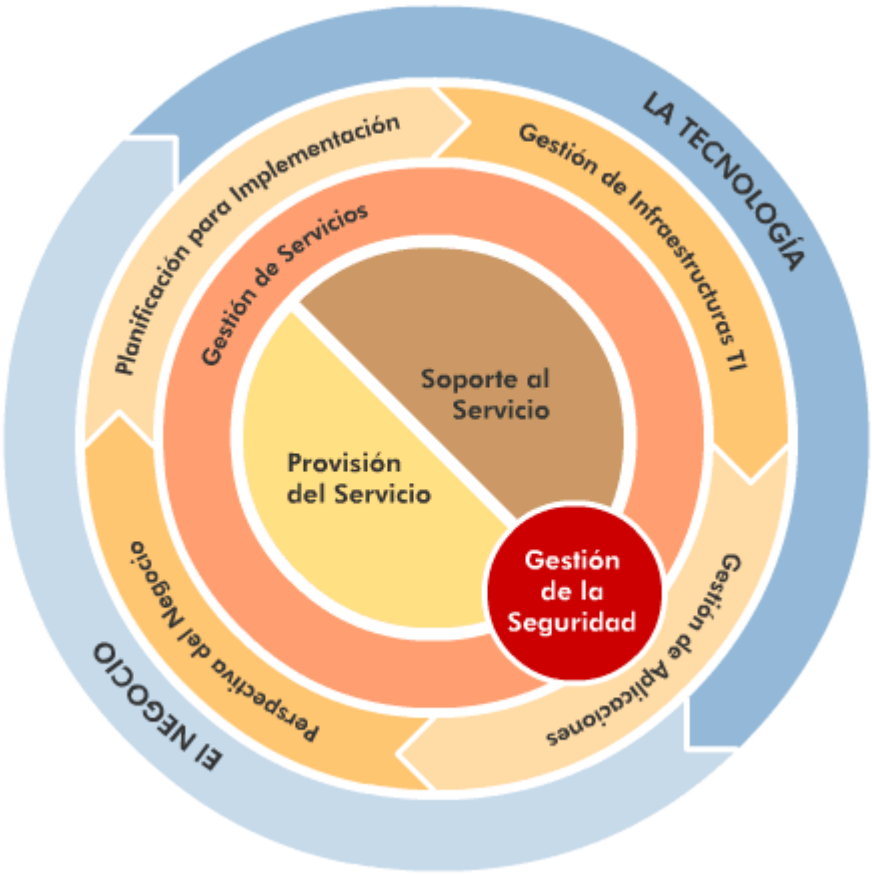

Figura 4. ITIL V3. - Tomada de itil.osiatis.es

ITIL busca asegurar la prestación de servicios de TI de alta calidad que satisfagan las necesidades de los usuarios y los requerimientos de la organización y cumplan

con las regulaciones aplicables. Estos servicios se deben entregar de forma eficiente y eficaz y deben ser revisados de forma continua para desarrollar actividades que permitan su mejoramiento.

Para una adecuada implementación de ITIL se requiere un conocimiento de los procesos de negocio, esto generaría grandes beneficios para la organización entre ellos:

- Servicios informáticos orientados al negocio
- Formaliza la prestación de los servicios de TI
- Mejora en la comunicación entre las áreas de negocio y la organización TI
- Uso efectivo y eficiente de las TI en el negocio
- Mejora las especificaciones de los servicios asegurando que estos cubran las necesidades del negocio
- Uso de TI para obtener una ventaja competitiva
- Mejora en la gestión de la calidad y los costos de los servicios de TI
- Identificar las relaciones en los procesos críticos
- Identificar áreas potenciales en los procesos para habilitar tecnologías
- Identificar oportunidades de "in-sourcing" y "outsourcing"

Así como COBIT define dominios ITIL define fases del ciclo de vida del servicio que contienen procesos. A continuación se listan los procesos para cada fase de ITIL:

Fase de Estrategia del Servicio: estrategia para el diseño, implementación, mantenimiento y mejora continua del servicio como una capacidad de la organización y un activo estratégico, entendiendo los planes del negocio para estructurar y ofrecer los servicios que brinden el valor necesario a los usuarios. Los procesos que lo componen son:

- Gestión Financiera
- Generación de la Estrategia

- Gestión de la Demanda
- Gestión de la Cartera de Servicios (SPM)

Fase de Diseño del Servicio: Documentación con todos los aspectos del servicio, así como los procesos que lo soportan. En esta etapa se establecen los elementos tecnológicos y los procesos que respondan a la estrategia planteada, a través del diseño de la arquitectura y las políticas de TI sobre el desarrollo de los servicios. Los procesos que lo componen son:

- Gestión del Catálogo de Servicios
- Gestión del Nivel de Servicio (SLM)
- Gestión de la Capacidad
- Gestión de la Disponibilidad
- Gestión de la Continuidad del Servicio TI (ITSCM)
- Gestión de la Seguridad de la Información
- Gestión de Suministradores

Fase de Transición del Servicio: Llevamos a cabo las estrategias planteadas y diseñadas, por medio de un plan de transición que incluye la infraestructura, el personal y los recursos. Se controlan los cambios a realizar para la operación del servicio y las relaciones entre los componentes. Los procesos que lo componen son:

- Planificación y Soporte de la Transición
- Gestión de Cambios
- Gestión de Configuración y Activos del Servicio SACM
- Gestión de Entregas y Despliegues
- Validación y pruebas del servicio
- Evaluación

- Gestión del Conocimiento

Fase de Operación del Servicio: Se refiere a la gestión y monitoreo de los servicios una vez puestos en el ambiente productivo, tal y como se definen en los Acuerdos de Niveles de Servicio; evaluando constantemente los eventos para garantizar que se mantengan estables y disponibles. Los procesos que lo componen son:

- Gestión de Eventos
- Gestión de Incidencias/Incidentes
- Gestión de Peticiones
- Gestión de Problemas
- Gestión de Accesos
- Service Desk (Centro de Servicio al Usuario) (Función)
- Gestión Técnica (Función)
- Gestión de la Operación de TI (Función)
- Gestión de Aplicaciones (Función)

Fase de Mejora Continua: Una vez que se pone en producción y se opera un servicio, nos enfocamos en un ciclo de mejoras continuas del mismo, a través de la medición e informes de gestión de los niveles de servicio y tomando en cuenta los beneficios del negocio, los métodos, las herramientas utilizadas, la identificación y la visión del servicio, a fin de diseñar estrategias acordes 100% a la organización. Los procesos que lo componen son:

- Medición del Servicio
- Proceso de mejora de CSI
- Informes de Servicio

5.4. ASPECTOS ARTICULADORES DE COBIT 4.1, ISO 27002 E ITIL V3

COBIT 4.1, ISO 27002 E ITIL V3 pueden ser articulados para la definición de un marco de un modelo de gobierno de TI. A través de las mejores prácticas las organizaciones pueden:

- Gestionar y controlar sus procesos y recursos
- Alinear sus objetivos con los del TI
- Priorizar proyectos y asignar los recursos necesarios para su ejecución
- Asignar responsables de los procesos y actividades del negocio y de TI
- Identificar riesgos de TI, asignar un responsable de su administración
- Implementar controles que mitiguen la probabilidad o impacto de los riesgos.
- Asegurar el uso eficiente de los recursos.
- Optimizar los costos.
- Garantizar capacidad suficiente para alcanzar los objetivos propuestos.
- Garantizar el retorno de la inversión
- Monitorear las actividades de TI y medir su cumplimiento.
- Cumplimiento de leyes y regulaciones aplicables.

EL gobierno de TI tiene 4 funciones primarias:

- Planeación y Alineamiento Estratégico (soportada por ITIL, COBIT)
- Operaciones de TI (soportada por ITIL, ISO/IEC 27002)
- Manejo Financiero (soportada por ITIL)
- Marcos de Control (soportada por COBIT, ISO/IEC 27002)

COBIT e ISO 27002 definen que se debe hacer mientras ITIL V3 como se debe hacer. COBIT es el estándar principal ya que provee un marco de control y gobierno basado en procesos de TI, mientras que ISO 27002 e ITIL V3 cubren

áreas específicas el primero la seguridad de la información y el segundo la gestión y soporte de servicios de TI.

Aspectos como la alineación de los objetivos TI con los del negocio permiten la articulación de COBIT e ITIL, los KGI y los criterios de información del marco de COBIT permiten definir los objetivos de TI, mientras ITIL definiendo niveles de servicio creando acuerdos de Nivel de que se ajusten a las necesidades del cliente.

COBIT e ITIL también pueden ser articulados en la identificación, definición y gestión de riesgos que afectan TI mientras que COBIT a través de su proceso de administración del Riesgo (PO9) permite la identificación de los riesgos y la asignación de responsables de su administración ITIL define los riesgos operacionales mientras ISO 27002 define los riesgos de seguridad de la información.

Otro aspecto en el que pueden ser articuladas estas mejores prácticas es en el análisis de la madurez de sus procesos haciendo uso de los modelos de madurez propuestos por COBIT e ITIL con el fin de identificar las mejoras necesarias.

6. DEFINICIÓN DE TÉRMINOS

- **Gobierno de TI:** conjunto de acciones que realiza el área de TI en coordinación con la alta dirección para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio.

- **Activo:** cualquier cosa que tenga valor para la organización.

- **Seguridad de Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Buenas prácticas:** Una forma aceptada por la industria de hacer algo, que funciona y mejora el resultado.

- **Metodología:** conjunto de procedimientos utilizados para alcanzar un objetivo

- **Información:** conjunto de datos procesados.

- **Marco de referencia:** conjunto de métodos y prácticas.

- **Norma:** principio que se adopta para dirigir la correcta realización de una acción.

7. ASPECTOS METODOLOGICOS

7.1. TIPO DE ESTUDIO

El tipo de estudio es investigativo-exploratorio ya que se realizo una investigación y exploración de las “mejores prácticas” que podían proporcionan lineamientos válidos para la construcción de un adecuado modelo de Gobierno de TI. Y a partir de esto construir una metodología que permite diagnosticar el estado de gobierno de tecnologías de la información de una organización.

7.2. METODO DE ESTUDIO

El método de investigación utilizado en este proyecto es inductivo.

7.3. TÉNICAS DE RECOLECCIÓN DE INFORMACIÓN

7.3.1. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN PRIMARIA

Se recolecto información del marco de referencia COBIT, las normas ISO 27001 e ISO 27002 e ITIL V 3.0

7.3.2. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN SECUNDARIA

Se hizo uso de páginas de Internet, tesis sobre gobierno de TI para obtener información relevante sobre el gobierno de tecnologías de la información.

8. RESULTADOS

La metodología propuesta para el diagnóstico de gobierno de tecnologías de la información fue diseñada tomando como base en el marco de referencia COBIT apoyado en la norma ISO 27002 y el estándar ITIL V3.0. Se han tomado estas 3 mejores prácticas por ser de amplio uso a nivel global, COBIT e ISO 27002 para ayudar a definir qué se debe hacer e ITIL para el cómo en lo referente a gestión de TI.

Un adecuado gobierno de TI requiere el uso e implementación de las mejores prácticas para la gestión de TI teniendo en cuenta esto se realizo la selección de estas 3 herramientas. Con ellas se busca garantizar una adecuada gestión de riesgos de TI, el cumplimiento de las regulaciones aplicables y la seguridad y continuidad de las operaciones de TI.

La alineación de estos 3 estándares se podría ver desde las 4 funciones primarias del gobierno de TI de la siguiente forma:

- Planeación y Alineamiento Estratégico (ITIL, COBIT)
- Operaciones de TI (ITIL, ISO/IEC 27002)
- Manejo Financiero (ITIL)
- Marcos de Control (COBIT, ISO/IEC 27002)

La metodología es general y aplicable a cualquier organización, consta de 8 fases o procedimientos los cuales no son de obligatoria aplicabilidad dependerá de la organización y el entorno en el que se aplique. A continuación se explicaran cada uno de estos procedimientos.

1. Conocimiento de la organización
2. Establecer el avance del medio
3. Selección de referentes conceptuales
4. Construcción del instrumento de recolección de información

5. Definición de métricas
6. Definición del nivel deseado
7. Aplicación del instrumento de recolección
8. Establecer la brecha entre el estado actual, el entorno y el estado deseado.

Conocimiento de la organización

Para lograr diagnosticar el estado de gobierno de TI se debe realizar una fase de reconocimiento de la organización, conociendo cada uno de los procesos que la componen, la interacción entre ellos. De igual forma, identificar su misión, visión, su actividad económica, el tipo de organización, su dimensión y por supuesto sus planes estratégicos tanto general como de tecnologías de la información. En esta fase se deberán solicitar algunos documentos a la organización como lo son:

- Mapa de procesos
- Misión, Visión, Objetivos, Metas, Políticas
- Mapa de Riesgos
- Plan estratégico
- Plan estratégico de TI
- Sistema de Gestión de la Seguridad de la Información

A su vez se deberá llevar a cabo una fase de observación del funcionamiento de los procesos de la organización así como entrevistas con personal clave dentro de la misma que puedan a partir de sus conocimientos y experiencias en el negocio aportar información relevante para el procedimiento.

Esta fase es el pilar de esta metodología ya que sin conocimientos de la organización no será posible establecer el personal clave de la organización, sus procesos misionales y los soportados por TI.

Establecer el estado del medio

Así como se realizó un procedimiento para conocer la organización, en este procedimiento se debe realizar un reconocimiento del entorno en el que se encuentra la organización, con el fin de conocer el estado actual del sector económico de la organización y determinar que organizaciones pueden tomarse como referencia para realizar comparaciones posteriormente.

Este proceso es importante ya que permitirá que más adelante la organización pueda conocer en qué nivel de madurez se encuentra su modelo de gobierno de TI con referencia a organizaciones con su misma actividad económica y a partir de esto tomar las medidas necesarias para mejorar las falencias que tenga el modelo implantado actualmente en la organización.

Esta es quizás la fase más difícil de la metodología ya que es difícil encontrar organizaciones que den a conocer su información a la competencia. Para llevar a cabo esta fase se recomienda realizar convenios con organizaciones del mismo sector, generando beneficios para las organizaciones del sector.

Este procedimiento se puede realizara través de entrevistas, observación y trabajo de campo en las organizaciones. Se deben diseñar y guardar todos los papeles de trabajo y documentación relevante de estas actividades como evidencias documentales, fotográficas, etc.

Selección de Referentes Conceptuales

Después de obtener conocimientos sobre la organización y su funcionamiento y del entorno en el cual se desarrolla, es necesario a partir de dicha investigación seleccionar los referentes conceptuales aplicables a la organización de acuerdo a sus necesidades, requerimientos, el contexto económico y social en el que se encuentre inmersa y las leyes aplicables.

Estos referentes conceptuales seleccionados deben ser utilizados en la construcción del patrón o instrumento de levantamiento de información que nos permitirá conocer el estado actual de la organización y a partir de este comparar la organización con el medio en el que se encuentra inmersa.

Para efectos generales se proponen como referentes COBIT como base para la creación del instrumento apoyado de las normas ISO 27001 e ITIL V3.0.

COBIT se tomo como base por ser un marco de referencia aceptado globalmente por las organizaciones para el gobierno de TI. Está basado en estándares y mejores prácticas, proporciona las herramientas para dirigir y supervisar las actividades propias de TI y las relacionadas con esta. También ayuda a aumentar el valor de TI a la organización mediante una adecuada gestión de las inversiones realizadas en TI.

ISO 27002 fue seleccionada para apoyar todo lo referente a seguridad de la información, para el desarrollo de un buen gobierno de TI garantiza la integridad, confidencialidad y disponibilidad de la información de la organización gestionada a través de recursos tecnológicos. Contar con un adecuado sistema de gestión de la seguridad de la información genera una ventaja competitiva para las organizaciones.

ITIL V3 como conjunto de mejores prácticas que busca prestar servicios de tecnología seguros, confiables, predecibles, sostenibles y eficientes, con un nivel de servicio adecuado a las necesidades del negocio, por ello es un referente necesario para el diagnostico del gobierno de TI de cualquier organización.

Construcción del instrumento de recolección de información

En esta fase de la metodología se deberá construir un instrumento para el levantamiento de información que permita medir el nivel de avance de gobierno de tecnologías de la información de la organización y su medio.

Este instrumento estará basado en los referentes conceptuales anteriormente seleccionados. Para la construcción del instrumento se recomienda analizar cada uno de los procesos definidos por COBIT con el fin de conocer el estado actual de cada uno para que se facilite la identificación de las falencias y así mismo realizar las recomendaciones pertinentes.

En los anexos de este proyecto encontraran un modelo de instrumento para el levantamiento de información en las organizaciones y su entorno.

La construcción de este instrumento hizo uso del modelo de madurez propuesto por COBIT para cada uno de los procesos que lo componen. Cada una de las preguntas da respuesta a uno de los niveles de cumplimiento propuestos por COBIT para los procesos. Estas preguntas dan respuesta a los objetivos de control de cada proceso, es decir las preguntas nacen de las metas de TI y los objetivos que se haya propuesto la organización. Aunque esta desarrollado de una forma general puede ser ajustado por cada organización de acuerdo a sus requerimientos y necesidades.

Definición de métricas

Luego de construir el instrumento para el levantamiento se deben definir unas métricas que permitan valorar de acuerdo a las respuestas del cuestionario el estado del gobierno de TI de la organización a la que se le aplique dicho instrumento.

Se debe definir un esquema de puntuación para las respuestas de cada una de las preguntas del instrumento de levantamiento de información, para el caso del

instrumento creado en este proyecto cada pregunta obedece a un nivel de cumplimiento. Con base a estas valoraciones se deben definir los niveles de madurez o cumplimiento en el caso de COBIT estos niveles son:

- 0 (No existente) → La empresa no ha reconocido sus problemas, no se evidencian procesos definidos.
- 1 (Inicial / Ad Hoc) → La empresa reconoce la existencia de problemas y la necesidad de solucionarlos pero no tiene procesos estándares.
- 2 (Repetible pero intuitivo) → La empresa ha desarrollado procesos sin embargo no se encuentran documentados, no han sido estandarizados ni comunicados al personal.
- 3 (Definido) → La empresa ha estandarizado sus procesos y han sido comunicados sin embargo, los individuos deciden si hacer uso de ellos o no.
- 4 (Administrado y Medible) → Los procedimientos se pueden medir, existen responsables de los mismos. De igual forma, se hace uso de la automatización en los procesos.
- 5 (Optimizado) → Los procesos hace uso de las mejores prácticas, están en mejoramiento continuo. Se usan indicadores de desempeño.

La escala utilizada debe ser granular porque dificultaría el diagnostico y requeriría una precisión exagerada para el fin que es detectar donde se encuentran las fallas dentro del modelo de gobierno de TI. Estas escalas deben definir estados actuales y futuros en los que la organización esta o desea estar.

Definición del nivel deseado

La organización deberá establecer cuál es el nivel de cumplimiento en el que desea estar, esto con el fin de que encamine sus esfuerzos y recursos para la

consecución de dicho nivel. Esto se debe convertir en un objetivo de la organización para garantizar el mejoramiento continuo de sus procesos.

El nivel deseado debe ser alcanzable y debe establecerse el periodo en el que la organización desea alcanzar dicho nivel a fin de realizar las actividades necesarias para la consecución del objetivo en el tiempo estipulado.

Aplicación del instrumento de recolección

En este procedimiento se procederá a aplicar el instrumento anteriormente desarrollado a personal clave de la empresa (dueños de procesos, auditores, usuarios finales, etc.) de acuerdo al proceso que se esté evaluando.

Para llevar a cabo esta fase se debe contar con apoyo y permisividad de la organización para realizar esta labor, ya que no solo consiste en responder las preguntas del instrumento, se debe realizar un análisis y revisión de evidencia que soporte las respuestas brindadas por el personal entrevistado.

Si no se cuenta con el permiso para acceder a la información necesaria para garantizar la veracidad de las respuestas, el estudio será en vano ya que carecerá de objetividad y lo más importante perderá total credibilidad y no garantizará que el resultado obtenido sea el estado actual de la organización.

Por ello se recomienda antes del inicio de esta metodología contar con el acceso irrestricto a la información de la organización. Lo ideal es replicar este procedimiento en organizaciones que realicen la misma actividad económica de la organización, que sean de la misma naturaleza y que se encuentren en el mismo entorno de esta. A continuación desarrollaremos a manera de ejemplo de la aplicación del instrumento de recolección que encuentra en el anexo de este proyecto.

DS13 – ADMINISTRAR LAS OPERACIONES			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Las actividades de soporte se encuentran definidas? ¿Las actividades de soporte satisfacen las necesidades de los niveles de servicio?	X	
2	¿Con qué frecuencia los equipos, sistemas y aplicaciones que soportan el negocio no se encuentran disponibles?	x	
3	¿Se encuentran documentadas las instrucciones de qué hacer, cuándo y en qué orden?		X
4	¿Los resultados de las actividades de soporte realizadas son registrados? ¿Se generan reporte de los incidentes y las actividades de soporte realizadas?	x	
5	¿Se ha definido un responsable de las operaciones de soporte?		X
6	¿Se realiza una programación de tareas? ¿Esta programación es comunicada al personal interesado?	x	
7	¿Con que frecuencia se reúne el personal de administración de operación con el de administración de cambios para garantizar la inclusión oportuna de cambios en producción?		X

R2:/ 1 o 2 veces al mes

Luego de aplicar el anterior cuestionario para medir el nivel de madurez del proceso DS13- Administrar las operaciones procedemos a tabular los resultados de la siguiente forma:

La primera y segunda pregunta obedecen al nivel 1, aunque realizan actividades de soporte, las aplicaciones no se encuentran disponibles 1 o 2 veces al mes, el sistema de la compañía no requiere una disponibilidad 7x24 de su sistema, pero sería crítico que en horario laboral se presentaran estos incidentes.

La tercera pregunta obedece al nivel 2 y también da respuesta al 3, al no estar documentadas las instrucciones de los procedimiento a realizar evidencian el no cumplimiento del 3 nivel y un gran porcentaje de cumplimiento con el nivel 2.

La cuarta pregunta obedece al nivel 3 se está haciendo registro de los incidentes y actividades realizadas. La quinta pregunta obedece al nivel 4 donde ya existen

responsables de los procedimientos, sin embargo, para el caso de esta compañía no existen responsables definidos claramente.

La pregunta 6 da respuesta al 4 nivel donde ya se realiza una programación de las labores y es comunicada al personal es decir que el proceso puede ser medido y valorado.

La pregunta 7 obedece al nivel 5 dando como resultado que no hace uso de las mejores prácticas del mercado que indica que para una adecuada administración de las operaciones se deben gestionar los cambios.

La información recolectada se puede tabular de la siguiente forma:

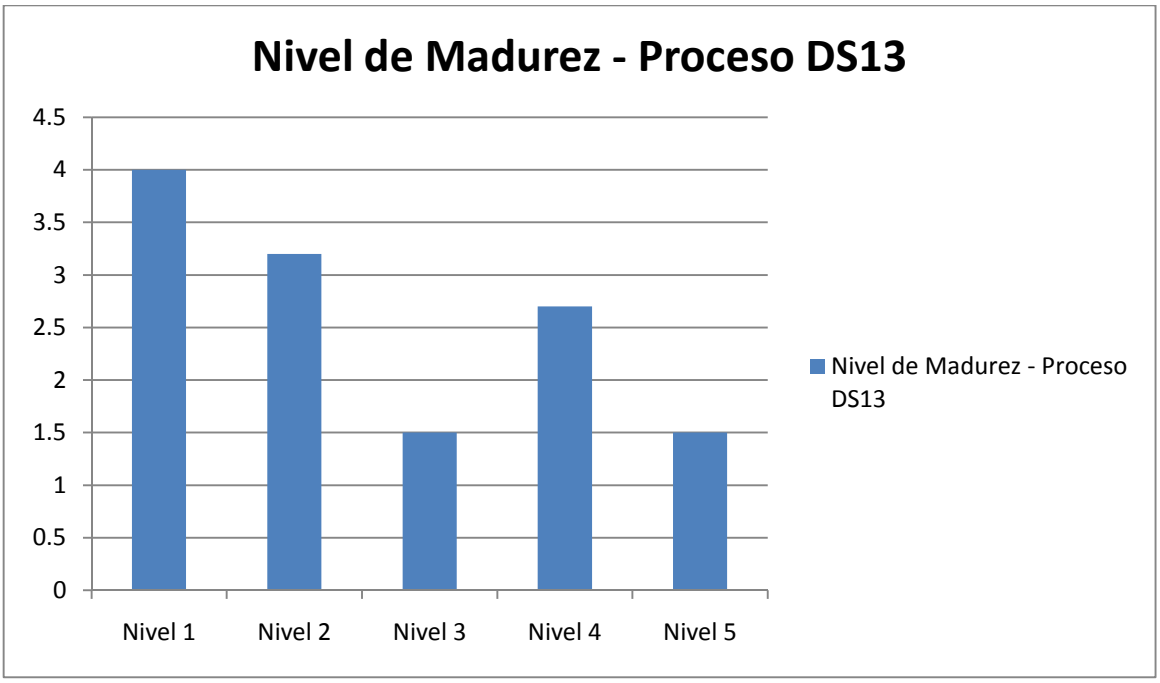

Figura 5. Gráfica Nivel de Madurez

Establecer la brecha entre el estado actual, el entorno y el estado deseado

Luego de aplicar el instrumento de levantamiento de información y aplicando el esquema de puntuación anteriormente establecido, se debe proceder a

contabilizar dichos puntos a fin de establecer el nivel de cumplimiento de gobierno de tecnologías de la información en que se encuentra la organización y las organizaciones de su entorno a las cuales se les haya aplicado el instrumento.

Con ello se debe proceder a realizar los comparativos entre el estado actual vs el deseado y el estado actual vs el promedio de la industria con el fin de establecer la brecha entre la organización y el mercado, así como, entre su estado actual y el deseado. A partir de este resultado se podrán definir y emprender las actividades necesarias para llegar a nivel deseado.

Siguiendo el ejemplo anterior y tomando como nivel deseado por al organización el nivel 4, que el promedio de la industria en 3 y que el proceso anterior dados los resultado se encuentra en un nivel entre 2 y 3 podríamos graficar nuestra brecha de la siguiente forma:

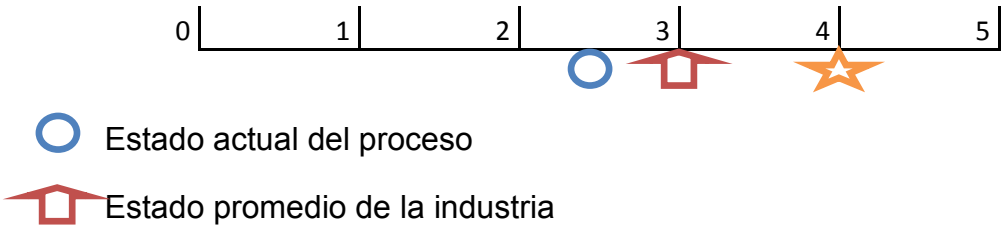

Figura 6. Comparación Nivel actual vs Nivel deseado Vs Nivel de la industria

Luego de identificar la brecha entre lo actual y lo deseado, y a ver detectado las falencias actuales del modelo de gobierno de TI de la organización, los directivos deberán definir y emprender actividades que permitan minimizar la brecha existente entre la organización y su nivel deseado. Si la organización se encuentra en el lugar deseado deberá entonces continuar con sus actividades pero consiente de que el entorno es cambiante y los riesgos evolucionan por tanto deberá mantener sus procesos en constante monitoreo para garantizar un mejoramiento continuo de sus procedimientos.

CONCLUSIÓN

Se puede concluir que existen estándares y normas que permiten diseñar un modelo de gobierno de tecnologías de la información y el desarrollo de una metodología para el diagnostico de dicho modelo. De igual forma, que COBIT es el referente conceptual más importante para el gobierno de tecnologías de la información de las organizaciones.

La metodología propuesta puede ser utilizada de acuerdo a las características y necesidades de las organizaciones para establecer el nivel de cumplimiento de su modelo de gobierno de tecnologías de la información. La metodología propuesta requiere del acceso irrestricto a la información de la organización a fin de generar un resultado integro y veraz, para esto la organización debe estar concientizada de la importancia de tener un adecuado modelo de gobierno de tecnologías de la información, conocer los beneficios de esta y su aporte en la toma de decisiones a la alta dirección.

El auditor encargado de diagnosticar deberá tener conocimiento de la organización y su entorno, deberá realizar su labor de forma objetiva y con total independencia, con el fin de garantizar la integridad de los resultados entregados a la organización para la toma de decisiones.

CRONOGRAMA DE ACTIVIDADES

ACTIVIDADES	JUL				AGO				SEP				OCT			
Identificación y selección de referentes conceptuales que soportarán el Proyecto																
Construcción del Instrumento para levantamiento de información en las empresas del Sector																
Fortalecimiento del Marco de Referencia COBIT para Gobierno de TI con los aportes de los referentes conceptuales seleccionados																
Diseño de la metodología para el diagnostico del estado de gobierno de TI.																
Documentación de la metodología diseñada																

BIBLIOGRAFIA

Sitio Web: http://moodle.bureauveritasformacion.com/file.php/23/UD01-REVISIoN_NORMA_ISO27001.pdf

Sitio Web: http://www.iso27000.es/iso27000.html#section3

Sitio Web: http://www.monografias.com/trabajos38/cobit/cobit2.shtml

Sitio Web: http://www.marblestation.com/?p=645

COBIT 4.1, ISACA – 2007

ITIL V3

Sitio Web: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php

ANEXOS

Instrumento para el levantamiento de información

PO → PLANEAR Y ORGANIZAR			
PO1 – DEFINIR UN PLAN ESTRATÉGICO DE TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿La gerencia de TI conoce la necesidad de una planeación estratégica de TI alineada con los objetivos corporativos?		
2	¿La planeación estratégica de TI sigue un enfoque estructurado, el cual se documenta y se da a conocer a todo el equipo?		
3	¿Existen procesos bien definidos para determinar el uso de recursos internos y externos requeridos en el desarrollo y las operaciones de los sistemas?		
4	¿Las consideraciones de riesgo y de valor agregado se actualizan de modo constante en el proceso de planeación estratégica de TI?		
5	¿Se realizan evaluaciones por comparación contra normas industriales bien entendidas y confiables y se integran con el proceso de formulación de la estrategia?		
PO2 – DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe conciencia de la importancia de la arquitectura de la información?		
2	¿La importancia de la arquitectura de la información se entiende y se acepta, y la responsabilidad de su aplicación se asigna y se comunica de forma clara?		
3	¿Se da soporte completo al desarrollo e implantación de la arquitectura de información por medio de métodos y técnicas formales?		
4	¿El personal de TI cuenta con la experiencia y las habilidades necesarias para desarrollar y dar mantenimiento a una arquitectura de información robusta y sensible que refleje todos los requerimientos del negocio?		
5	¿Se hace un uso amplio de las mejores prácticas de la industria en el desarrollo y mantenimiento de la arquitectura de información incluyendo un proceso de mejora continua?		
PO3 – DETERMINAR LA DIRECCIÓN TECNOLÓGICA			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe conciencia sobre la importancia de la planeación de la infraestructura tecnológica para la entidad?		

2	¿Existe un plan de infraestructura tecnológica definido, documentado y bien difundido?		
3	¿La responsabilidad del desarrollo y mantenimiento del plan de infraestructura tecnológica han sido asignados?		
4	¿Se han incluido buenas prácticas internas en el proceso?		
5	¿Existe una función de investigación que revisa las tecnologías emergentes y evolutivas y para evaluar la organización por comparación contra las normas industriales?		
PO4 – DEFINIR LOS PROCESOS, ORGANIZACIÓN Y RELACIONES DE TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existen roles y responsabilidades definidos para la organización de TI y para terceros?		
2	¿La organización de TI se desarrolla, documenta, comunica y se alinea con la estrategia de TI y se define el ambiente de control interno?		
3	¿La administración, la propiedad de procesos, la delegación y la responsabilidad de TI están definidas y balanceadas?		
4	¿La gerencia de TI cuenta con la experiencia y habilidades apropiadas para definir, implantar y monitorear la organización deseada y las relaciones?		
5	¿Se ponen en funcionamiento las mejores prácticas de la industria y existe un uso amplio de la tecnología para monitorear el desempeño de la organización y de los procesos de TI?		
PO5 – ADMINISTRAR LA INVERSIÓN EN TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un entendimiento de la necesidad de seleccionar y presupuestar y comunicar las inversiones?		
2	¿Las políticas y los procesos para inversiones y presupuestos están definidas, documentadas y comunicadas y cubren temas clave de negocio y de tecnología?		
3	¿El presupuesto de TI está alineado con los planes estratégicos de TI y con los planes del negocio?		
4	¿Se utilizan las mejores prácticas de la industria para evaluar los costos por comparación e identificar la efectividad de las inversiones?		
5	¿Se incluye un análisis de los costos y beneficios a largo plazo del ciclo de vida total en la toma de decisiones de inversión?		
PO6 – COMUNICAR LAS ASPIRACIONES Y LA DIRECCIÓN DE LA GERENCIA			
N°	**PREGUNTA**	**SI**	**NO**
1	¿La gerencia es reactiva al resolver los requerimientos del ambiente de control de información?		
2	¿La gerencia tiene un entendimiento de las necesidades y de los requerimientos de un ambiente de control de información		

	efectivo?		
3	¿El proceso de elaboración de políticas es estructurado, mantenido y conocido por el personal?		
4	¿El ambiente de control de la información está alineado con el marco administrativo estratégico y con la visión, y con frecuencia se revisa, actualiza y mejora?		
5	¿Se asignan expertos internos y externos para garantizar que se adoptan las mejores prácticas de la industria, con respecto a las guías de control y a las técnicas de comunicación?		
PO7 – ADMINISTRAR RECURSOS HUMANOS DE TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe conciencia sobre la importancia de alinear la administración de recursos humanos de TI con el proceso de planeación de la tecnología para la organización?		
2	¿El proceso de recursos humanos de TI está enfocado de manera operacional en la contratación y administración del personal?		
3	¿Existe un proceso definido y documentado para administrar los recursos humanos y un enfoque estratégico para la contratación y la administración del personal de TI?		
4	¿La organización cuenta con métricas estandarizadas que le permiten identificar desviaciones respecto al plan de administración de recursos humanos de TI?		
5	¿Los componentes de la administración de recursos humanos de TI son consistentes con las mejores prácticas de la industria, tales como compensación, revisiones de desempeño, participación en foros de la industria, transferencia de conocimiento, entrenamiento y adiestramiento?		
PO8 – ADMINISTRAR LA CALIDAD			
N°	**PREGUNTA**	**SI**	**NO**
1	¿La alta dirección y el equipo de TI no reconocen que un programa de calidad es necesario?		
2	¿Se establece un programa para definir y monitorear las actividades de QMS dentro de TI?		
3	¿Se usan métodos de análisis de costo/beneficio para justificar las iniciativas de QMS?		
4	¿Los procesos de QMS son flexibles y adaptables a los cambios en el ambiente de TI y mejora la base de conocimientos para métricas de calidad con las mejores prácticas externas?		
5	¿Se realiza benchmarking contra estándares externos rutinariamente?		
PO9 – EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI			
N°	**PREGUNTA**	**SI**	**NO**

1	¿Se realiza la evaluación de riesgos para los procesos y las decisiones de negocio?		
2	¿Se tienen en cuenta los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad proyecto por proyecto?		
3	¿La captura, análisis y reporte de los datos de administración de riesgos están altamente automatizados?		
4	¿La administración de riesgos está altamente integrada en todo el negocio y en las operaciones de TI está bien aceptada, y abarca a los usuarios de servicios de TI?		
5	¿La dirección evalúa las estrategias de mitigación de riesgos de manera continua?		
PO10 – ADMINISTRAR PROYECTOS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe compromiso por parte de la gerencia hacia la propiedad de proyectos y hacia la administración de proyectos?		
2	¿El proceso y la metodología de administración de proyectos de TI han sido establecidos y comunicados?		
3	¿Se han establecido los criterios para evaluar el éxito en cada punto clave?		
4	¿El valor y el riesgo se miden y se administran, antes, durante y al final de los proyectos?		
5	¿La planeación de programas y proyectos en toda la organización garantiza que los recursos de TI y del usuario se utilizan de la mejor manera para apoyar las iniciativas estratégicas?		
AI → ADQUIRIR E IMPLEMENTAR			
AI1 – IDENTIFICAR SOLUCIONES AUTOMATIZADAS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas?		
2	¿Existe una metodología clara para la identificación y la evaluación de las soluciones de TI y se usa para la mayoría de los proyectos?		
3	¿Existe interfaz definida de forma clara entre la gerencia de TI y la del negocio para la identificación y evaluación de las soluciones de TI?		
4	¿Se identifican nuevas oportunidades de uso de la tecnología para ganar una ventaja competitiva, ejercer influencia en la re-ingeniería de los procesos de negocio y mejorar la eficiencia en general?		
AI2 – ADQUIRIR Y MANTENER SOFTWARE APLICATIVO			

N°	PREGUNTA	SI	NO
1	¿Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones?		
2	¿Existe un proceso claro, definido y de comprensión general para la adquisición y mantenimiento de software aplicativo?		
3	¿Las actividades de mantenimiento se planean, programan y coordinan?		
4	¿Existe una metodología formal y bien comprendida que incluye un proceso de diseño y especificación, un criterio de adquisición, un proceso de prueba y requerimientos para la documentación?		
5	¿Existen mecanismos de aprobación documentados y acordados, para garantizar que se sigan todos los pasos y se autoricen las excepciones?		
AI3 – ADQUIRIR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Se reconoce la administración de la infraestructura de tecnología como un asunto importante al cual deba ser resuelto?		
2	¿Existe un claro, definido proceso para adquirir y dar mantenimiento a la infraestructura TI?		
3	¿El proceso de adquisición y mantenimiento de la infraestructura de tecnología es preventivo y está estrechamente en línea con las aplicaciones críticas del negocio y con la arquitectura de la tecnología?		
4	¿Se siguen buenas prácticas respecto a las soluciones de tecnología, y la organización tiene conciencia de las últimas plataformas desarrolladas y herramientas de administración?		
5	¿Se reducen costos al racionalizar y estandarizar los componentes de la infraestructura y con el uso de la automatización?		
AI4 – FACILITAR LA OPERACIÓN Y EL USO			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Los procedimientos se encuentran disponibles fuera de línea y se pueden acceder y mantener en caso de desastre?		
2	¿Se utilizan herramientas automatizadas en la generación y distribución de procedimientos?		
3	¿Existe un esquema definido para los procedimientos de mantenimiento y para los materiales de entrenamiento que cuentan con el soporte de la administración de TI?		
4	¿El desarrollo de materiales de documentación y entrenamiento como la entrega de programas de entrenamiento, se encuentran completamente integrados con el negocio y con las definiciones		

	de proceso del negocio?		
AI5 – ADQUIRIR RECURSOS DE TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un proceso definido de adquisición de recursos de TI?		
2	¿La organización ha reconocido la necesidad de tener políticas y procedimientos documentados que enlacen la adquisición de TI con el proceso general de adquisiciones de la organización?		
3	¿Se determinan responsabilidades y rendición de cuentas para la administración de adquisición y contrato de TI según la experiencia particular del gerente de contrato?		
4	¿Existen estándares de TI para la adquisición de recursos de TI y los proveedores de recursos de TI?		
5	¿La administración de TI comunica la importancia estratégica de tener una administración apropiada de adquisiciones y contratos, a través de la función TI?		
AI6 – ADMINISTRAR CAMBIOS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Hay conciencia de que el cambio puede causar una interrupción para TI y las operaciones del negocio y de los beneficios de la buena administración de cambio?		
2	¿Existe un proceso formal definido para la administración del cambio, que incluye la categorización, asignación de prioridades, procedimientos de emergencia, autorización del cambio?		
3	¿Se da un proceso de aprobación para cambios?		
4	¿Hay un proceso consistente para monitorear la calidad y el desempeño del proceso de administración de cambios?		
5	¿El proceso de administración de cambios se revisa con regularidad y se actualiza para permanecer en línea con las buenas prácticas?		
AI7 – INSTALAR Y ACREDITAR SOLUCIONES Y CAMBIOS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe consistencia entre los enfoques de prueba y acreditación?		
2	¿Los procesos de TI para instalación y acreditación están integrados dentro del ciclo de vida del sistema y están automatizados?		
3	¿El sistema de prueba refleja adecuadamente el ambiente de producción?		
4	¿Los procesos de TI para la instalación y acreditación están totalmente integrados dentro del ciclo de vida del sistema y se automatizan cuando es apropiado, arrojando el estatus más eficiente de entrenamiento, pruebas y transición a producción		

	para los nuevos sistemas?		
5	¿Los ambientes de prueba bien desarrollados, los registros de problemas y los procesos de resolución de fallas aseguran la transición eficiente y efectiva al ambiente de producción?		
DS → ENTREGAR Y DAR SOPORTE			
DS1 – DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un proceso que defina y administre los niveles de servicio del departamento de TI?		
2	¿Se han asignado responsables de la administración de los niveles de servicios?		
3	¿El proceso de administración de los niveles de servicios ha sido comunicado a la organización?		
4	¿Los servicios y niveles de servicio se encuentran documentados?		
5	¿Qué herramientas son utilizadas para la administración de los niveles de servicio? ¿Son automatizadas?		
6	¿Se monitorea, evalúa y generan reportes del proceso de administración de los niveles de servicio?		
DS2 – ADMINISTRAR LOS SERVICIOS DE TERCEROS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existen políticas y procedimientos para la contratación de terceros?		
2	¿Se han asignado responsables de la supervisión de los servicios prestados por terceros?		
3	¿Las partes involucradas tienen conocimientos de los costos, etapas y expectativas del servicio?		
4	¿Los procedimientos para la contratación y control los servicios prestados por terceros se encuentran documentados?		
5	¿En el acuerdo contractual se incluye el alcance del trabajo, los servicios a suministrar, entregables, costos, cronograma, acuerdos de facturación?		
6	Se han identificado los riesgos asociados a la contratación de terceros? ¿Son valorados? ¿Son evaluados y monitoreados?		
7	¿Está definida una periodicidad para la revisión del contrato y el monitoreo del cumplimiento de las condiciones operativas, legales y de control definidas en el mismo?		
DS3 – ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Se realiza un proceso de planeación de la capacidad y el desempeño?		
2	¿Cuál es el nivel de satisfacción de los usuarios con respecto la capacidad del servicio actual? ¿Pueden solicitar nuevos		

	servicios?		
3	¿Los requerimientos de desempeño y capacidad están definidos a lo largo del ciclo de vida del sistema?		
4	¿Se hace una evaluación de la capacidad de desempeño de TI? ¿Se consideran situaciones de peor-escenario?		
5	¿Existen procesos estandarizados para enfrentar fallas por desempeño o capacidad?		
6	¿Se generan reportes con estadísticas de desempeño?		
7	¿Los planes de capacidad y desempeño están sincronizados con las proyecciones de demanda del negocio?		
DS4 – GARANTIZAR LA CONTINUIDAD DEL SERVICIO			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un plan de continuidad? ¿Está documentado?		
2	¿Las pruebas de continuidad están definidas? ¿Existen responsables? ¿Existen reportes periódicos? ¿Son utilizadas en la actualización del plan de continuidad?		
3	¿El personal sigue estándares y se capacita para enfrentarse con incidentes mayores o desastres?		
4	¿Se han aplicado componentes de alta capacidad y rendimiento?		
5	¿Se implementan buenas prácticas de disponibilidad de los sistemas?		
6	¿El plan de continuidad de IT se encuentra integrado con el plan de continuidad del negocio?		
7	¿Se le realiza mantenimiento al plan de continuidad?		
DS5 – GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un proceso de respuesta para resolver problemas de seguridad de TI? ¿Quiénes lo ejecutan?		
2	¿Es analizada la información respecto a la seguridad arrojada por los sistemas de información?		
3	¿Se han definido políticas de seguridad de la información? ¿Son aplicadas por el personal?		
4	¿Se realizan pruebas de seguridad de TI?		
5	¿Se encuentran certificados a nivel de seguridad de TI? En caso de no contar con ella ¿Están en busca de ella?		
6	¿Los usuarios están concientizados y comprometidos con las políticas de seguridad de TI? ¿Se responsabilizan de los requerimientos se seguridad de la información que manejan?		
7	¿Con qué periodicidad se evalúa la efectividad del plan de seguridad de TI?		
DS6 – IDENTIFICAR Y ASIGNAR COSTOS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un proceso de identificación y distribución de costos de		

	TI?		
2	¿Se ha asignado un responsable de la asignación de costos?		
3	¿Existe un monitoreo y evaluación de los costos? ¿Se utiliza para optimizar los costos de recursos de TI?		
4	¿Los reportes de costos están ligados a los niveles de servicio y a los objetivos del negocio? ¿Son revisados y vigilados por los dueños de procesos de negocio?		
5	¿Existe un proceso automático de distribución de costos? ¿Se enfoca en los servicios de información o en el negocio en general?		
6	¿Existe un proceso que relacione los costos de TI con los servicios prestados?		
DS7 – EDUCAR Y ENTRENAR A LOS USUARIOS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿La compañía cuenta con programas de entrenamiento y capacitación a los usuarios? ¿Con que periodicidad se realizan? ¿Cuál es el contenido de estos programas?		
2	¿Los procesos de entrenamiento se encuentran documentados y estandarizados?		
3	¿Los procesos de entrenamiento son monitoreados y evaluados?		
4	¿Se ha asignado un responsable del proceso de entrenamiento y capacitación?		
5	¿Los programas de entrenamiento hacen parte del plan de carrera de los empleados?		
6	¿TI es utilizada como herramienta en los procesos de entrenamiento y capacitación?		
DS8 – ADMINISTRAR LA MESA DE SERVICIO Y LOS INCIDENTES			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un proceso de administración de incidentes? ¿El departamento de TI cuenta con una mesa de ayuda?		
2	¿El personal de la mesa de ayuda cuenta con herramientas que le permiten resolver los incidentes?		
3	¿Los procedimientos para la solucionar de incidentes se encuentran documentados y estandarizados?		
4	¿Existen guías de usuario y preguntas frecuentes (FAQs)? ¿Son de fácil acceso para los usuarios?		
5	¿Las consultas de usuarios, incidentes y tendencias son monitoreados y revisados?		
6	¿Se han desarrollado indicadores de desempeño para medir el rendimiento de la mesa de servicio?		
DS9 – ADMINISTRAR LA CONFIGURACIÓN			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existe un proceso que permita administrar la configuración de		

	la infraestructura TI, tanto hardware como software?		
2	¿El proceso de administración de la configuración se encuentra documentado y estandarizado?		
3	¿Qué herramientas son utilizadas para la administración de la configuración? ¿Estas herramientas son similares entre plataformas o difieren en su totalidad?		
4	¿Los reportes de auditoría brindan informe esencial sobre el software y hardware con respecto a reparaciones, servicios, garantías, evaluaciones técnicas?		
5	¿Las desviaciones son monitoreadas, rastreadas y reportadas?		
6	¿Qué porcentaje de los activos de TI cubren los sistemas de administración de la configuración?		
DS10 – ADMINISTRAR LOS PROBLEMAS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existen responsables para la administración de problemas?		
2	¿Existe un proceso que permita administrar problemas y resolver las causas de fondo?		
3	¿Se realizan revisiones del proceso de administración de riesgos?		
4	¿Los problemas se encuentran identificados, registrados y documentados?		
5	¿La administración de problemas está integrada con los procesos interrelacionados como la administración de incidentes, cambios, y configuración?		
6	¿El proceso de administración de problemas es proactivo y preventivo?		
7	¿Los sistemas están equipados con mecanismos automáticos de advertencia y detección?		
DS11 – ADMINISTRAR LOS DATOS			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Se ha definido responsables de la administración de los datos?		
2	¿Existen procedimientos de respaldo y recuperación de datos?		
3	¿Se encuentran definidos los propietarios o responsables de los datos?		
4	¿Se realiza algún tipo de monitoreo sobre las actividades de administración de datos (respaldo, recuperación y eliminación)?		
5	¿Los procedimientos de administración e datos esta formalizados dentro de TI?		
6	¿Qué herramientas son utilizadas en la administración de datos?		
7	¿Los requerimientos de seguridad para la administración de datos es documentada por personal clave?		
DS12 – ADMINISTRAR EL AMBIENTE FISICO			
N°	**PREGUNTA**	**SI**	**NO**

1	¿Existen controles ambientales contra peligros naturales y causados por el hombre? ¿Quiénes son los encargados de su implementación y monitoreo?		
2	¿Existen procedimientos para el mantenimiento de las instalaciones? ¿De quienes depende? ¿Se encuentran documentados? ¿Están estandarizados?		
3	¿La seguridad física, el mantenimiento físico y los controles ambientales tienen asignado un presupuesto?		
4	Se han definido planes de mantenimiento preventivo? ¿Con que periodicidad se realizan? ¿Se realizan horarios preestablecidos? ¿Se realizan con mayor regularidad a equipos sensibles?		
5	¿Se realiza inventario de todas las instalaciones realizadas de acuerdo con el proceso de administración de riesgos?		
6	¿El acceso de personal es monitoreado constantemente?		
7	¿Se aplican restricciones de acceso al centro de cómputo? ¿Los visitantes se registran y acompañan dependiendo del individuo o son acompañados en todo momento?		
DS13 – ADMINISTRAR LAS OPERACIONES			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Las actividades de soporte se encuentran definidas? ¿Las actividades de soporte satisfacen las necesidades de los niveles de servicio?		
2	¿Con qué frecuencia los equipos, sistemas y aplicaciones que soportan el negocio nos e encuentran disponibles?		
3	¿Se encuentran documentadas las instrucciones de qué hacer, cuándo y en qué orden?		
4	¿Los resultados de las actividades de soporte realizadas son registrados?¿Se generan reporte de los incidentes y las actividades de soporte realizadas?		
5	¿Se ha definido un responsable de las operaciones de soporte?		
6	¿Se realiza una programación de tareas? ¿Esta programación es comunicada al personal interesado?		
7	¿Con que frecuencia se reúne el personal de administración de operación con el de administración de cambios para garantizar la inclusión oportuna de cambios en producción?		
ME → MONITOREAR Y EVALUAR			
ME1 – MONITORER Y EVALUAR EL DESEMPEÑO DE TI			
N°	**PREGUNTA**	**SI**	**NO**
1	¿La organización cuenta con un proceso de monitoreo?		
2	¿El monitoreo se encuentra implantado o se realiza cuando ocurren incidentes que ha ocasionado pérdidas a la organización?		
3	¿Se recolecta información del proceso de monitoreo para su		

	posterior evaluación? ¿Existe un método o técnica para la recolección de información? ¿Ha sido adoptada por toda la organización?		
4	¿Las evaluaciones se realizan a nivel de procesos y proyectos individuales de TI o a nivel de los procesos en general?		
5	¿Se han definido herramientas para realizar el monitoreo de los procesos y los niveles de servicio de TI?		
6	¿Se han definido mediciones del nivel de satisfacción de los usuarios, del desempeño de TI, las estrategias y los niveles de servicio?		
7	¿Las herramientas automatizadas son utilizadas en todos los niveles de la organización para monitorear y recolectar la información de los procesos, sistemas y aplicaciones?		
ME2 – MONITORERA Y EVALUAR EL CONTROL INTERNO			
N°	**PREGUNTA**	**SI**	**NO**
1	¿La organización cuenta con procedimientos para el monitoreo del control interno?		
2	¿Se han definido responsables del monitoreo de la efectividad del control interno?		
3	¿Las evaluaciones de control interno de TI se realizan como parte de las auditorías internas tradicionales?		
4	¿Se utiliza metodologías y herramientas para realizar el monitoreo de los controles internos?		
5	¿El monitoreo de controles internos esta institucionalizado?		
6	¿Se ha definido un proceso de autoevaluaciones y revisiones de aseguramiento del control interno? ¿Quiénes son los encargados de realizar la evaluación de control interno de TI?		
7	¿Existe una base de datos de métricas para información histórica sobre el monitoreo de control interno?		
ME3 – GARANTIZAR EL CUMPLIMIENTO REGULATORIO			
N°	**PREGUNTA**	**SI**	**NO**
1	¿Existen procesos para mantener el cumplimiento de requisitos legales, contractuales y regulatorios? ¿Estos se siguen con regularidad o en respuesta a auditorias o revisión? ¿Han sido comunicadas a todos los niveles de la organización? ¿Se encuentran actualizadas?		
2	¿Se realiza capacitación y entrenamiento sobre regulaciones y leyes externas aplicables a la organización?		
3	¿Se realiza monitoreo sobre el cumplimiento de leyes y regulaciones? ¿Existen requisitos de cumplimiento que no han sido resueltos?		
4	¿Existe contratos pro forma y procesos legales estándar para minimizar el riesgo contractual?		
ME4 – PROPORCIONAR GOBIERNO DE TI			

N°	PREGUNTA	SI	NO
1	¿Existen procesos de planeación, entrega y supervisión de TI?		
2	¿Los procesos de gobierno de TI son monitoreados?		
3	¿Se han asignado los responsables y dueños de cada proceso?		
4	¿Los empleados impulsan los procesos de gobierno en procesos y proyectos de TI?		
5	¿Se han seleccionado procesos de TI para su mejoramiento?		
6	¿Se han implementado herramientas para el manejo y control del gobierno de TI?		
7	¿Existen indicadores de desempeño para los procesos de gobierno de TI? ¿Se encuentran registrados?		
8	¿EL personal se ha adaptado a la implementación de gobierno de TI?		

ANEXO B
CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS Y TRABAJOS DE GRADO

Barranquilla, Octubre 25 de 2011

Marque con una X
Tesis [ ] **Trabajo de Grado** [x]

Yo Derlys Katherine Navas Lineros, identificado con C.C. No. 1129569896, actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado "Diseño de una metodología para realizar diagnóstico al estado de gobierno de ti en una organización fundamentado en los lineamientos establecidos por los estándares reconocidos como las mejores prácticas" presentado y aprobado en el año 2011 como requisito para optar al título de Especialista en Auditoria de Sistemas de Información;
hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Corporación Universitaria de la Costa, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los 25 días del mes de Octubre de Dos Mil Once 2011

EL AUTOR - ESTUDIANTE._____

FIRMA

ANEXO C
FORMULARIO DE LA DESCRIPCIÓN DE LA TESIS O DEL TRABAJO DE GRADO

TÍTULO COMPLETO DE LA TESIS O TRABAJO DE GRADO: "Diseño de una metodología para realizar diagnóstico al estado de gobierno de ti en una organización fundamentado en los lineamientos establecidos por los estándares reconocidos como las mejores prácticas"

SUBTÍTULO, SI LO TIENE:

_____

AUTOR AUTORES

Apellidos Completos	Nombres Completos
Navas Lineros	Derlys Katherine

DIRECTOR (ES)

Apellidos Completos	Nombres Completos
Montaño Ardila	Víctor Manuel

JURADO (S)

Apellidos Completos	Nombres Completos

ASESOR (ES) O CODIRECTOR

Apellidos Completos	Nombres Completos

TRABAJO PARA OPTAR AL TÍTULO DE: Especialista en Auditoria de Sistemas de Información

FACULTAD: Ciencias Económicas

PROGRAMA: Pregrado ____ Especialización _X__

NOMBRE DEL PROGRAMA: Especialización en Auditoría de Sistemas de Información

CIUDAD: Barranquilla **AÑO DE PRESENTACIÓN DEL TRABAJO DE GRADO:** 2011

NÚMERO DE PÁGINAS ___60_____

TIPO DE ILUSTRACIONES:

- ☐ Ilustraciones
- ☐ Láminas
- ☐ Retratos
- ☒ Tablas, gráficos y diagramas
- ☐ Planos
- ☐ Mapas
- ☐ Fotografías

MATERIAL ANEXO (Vídeo, audio, multimedia o producción electrónica):

Duración del audiovisual: _____ minutos.

Número de casetes de vídeo: _____ Formato: VHS ___ Beta Max ___ ¾ ___ Beta Cam ____

Mini DV ____ DV Cam ____ DVC Pro ____ Vídeo 8 ____ Hi 8 ____

Otro. Cuál? _____

Sistema: Americano NTSC _____ Europeo PAL _____ SECAM _____

Número de casetes de audio: _____

Número de archivos dentro del DVD (En caso de incluirse un DVD diferente al trabajo de grado):

_____

PREMIO O DISTINCIÓN *(En caso de ser LAUREADAS o tener una mención especial)*:

_____

DESCRIPTORES O PALABRAS CLAVES EN ESPAÑOL E INGLÉS: Son los términos que definen los temas que identifican el contenido. (*En caso de duda para designar estos descriptores, se recomienda consultar con la Unidad de Procesos Técnicos de la Unidad de información en el correo biblioteca@cuc.edu.co, donde se les orientará).*

ESPAÑOL	**INGLÉS**
Gobierno de TI	IT Governance
Modelo de Madurez	Maturity Model

RESUMEN DEL CONTENIDO EN ESPAÑOL E INGLÉS:(Máximo 250 palabras-1530 caracteres):

En este proyecto se propone una metodología para diagnosticar el estado actual del gobierno de TI de una organización con el fin de conocer el nivel de madurez y cumplimiento de la organización con respecto al modelo que ha establecido. Para el desarrollo de la misma se toma como base el marco de referencia COBIT a

partir de estos se diseñó un instrumento de levantamiento de información sencillo que permitirá valorar de forma general el modelo de gobierno de cualquier organización.

La metodología propuesta consta de 8 fases partiendo del conocimiento de la organización y su entorno, siguiendo por la selección de referentes conceptuales que serán utilizados en la creación del instrumento de levantamiento de la organización. La organización deberá establecer un esquema de puntuación y unas métricas para valorar los resultados de la aplicación del instrumento. Luego de la aplicación del instrumento y su valoración se procederá a establecer la brecha existente entre el estado actual de la organización y su estado deseado y entre el estado de la organización y el de su entorno. El diagnostico permitirá definir e implementar las actividades y procedimientos necesarios para lograr alcanzar el nivel deseado por la organización.

SUMMARY

This project proposes a methodology to diagnose the current state of IT governance in an organization to know the level of maturity and performance of the organization with respect to the model set. For the development of it is taken based on the COBIT framework from these an instrument was designed to gather information that will evaluate simple generally the governance of any organization.

The proposed methodology consists of 8 phases from knowledge about the organization and its environment, following the selection of conceptual references that will be used in creating the survey instrument of the organization. The organization shall establish a scoring scheme and a metric to assess the results of applying the instrument. After application of the instrument and its evaluation will proceed to establish the gap between the current state of the organization and its

desired state and between the state of the organization and its environment. The diagnosis will define and implement activities and procedures necessary to achieve the desired level by the organization.